Data sheet

HP 10500/7500 20G Unified Wired-WLAN TAA-compliant Module

Key features

- Enterprise-scale capacity, performance, and high reliability for wireless networks
- System-wide approach to WLAN reliability through Wi-Fi Clear Connect
- Flexible forwarding modes
- Comprehensive feature set for demanding Enterprise environments

Product overview

The IEEE 802.11ac-ready HP 10500/7500 20G Unified Wired-WLAN TAA-compliant Module delivers enterprise-scale features, capacity up to 1024 APs and 20G of centralized throughput, and high reliability, as well as offering substantial data processing capacity for wireless networks requiring TAA-compliant products. The module can operate in the HP 11900, 10500, and 7500 Switch Series and supports IEEE 802.11a/b/g/n and IEEE 802.11ac APs and access devices.

The HP 10500/7500 20G Unified Wired-WLAN TAA-compliant Module provides refined user control and management, comprehensive RF management and security mechanisms, fast roaming, QoS and IPv4/IPv6 features, and powerful WLAN access control.

Designed for the WLAN access of enterprise networks, this module provides an industry-leading WLAN solution for large enterprise networks. Working together with HP access points, the HP 10500/7500 Unified Wired-WLAN Module can be easily deployed on Layer 2 or Layer 3 networks without affecting existing configurations.

Features and benefits

Management

• Wi-Fi Clear Connect

provides a system-wide approach to help ensure WLAN reliability by proactively determining and adjusting to changing RF conditions and by identifying rogue activity and enforcing prevention, and optimizing WLAN performance by detecting interference from Wi-Fi and non-Wi-Fi sources using spectrum analysis capabilities built into specific access points (refer to the HP Access Point—Controller Compatibility Matrix for specific access points supported).

• Advanced radio resource management

– Automatic radio power adjustments

includes real-time power adjustments based on changing environmental conditions and signal coverage adjustment

– Automatic radio channel

provides intelligent channel switching and real-time interference detection

– Intelligent client load balancing

balances the number of clients across multiple APs to optimize AP and client throughput

– Airtime fairness

helps ensure equal RF transmission time for wireless clients

• Spectrum analysis

– Signal detection/classification

identifies source of RF interference, for example, Bluetooth®, cordless phones, and microwave ovens

– Evaluation of channel quality

helps detect severe channel degradation and improves the reporting of poor RF performance

• Band navigation

enables automatic redirection of 5 GHz-capable clients to the less-congested 5 GHz spectrum

• Enterprise network management

is provided by HP Intelligent Management Center (IMC) Platform Software and the IMC Wireless Services Manager Software Module, which effectively integrate traditionally disparate management tools into one easy-to-use interface

• Secure controller management

securely manages the controller from a single location with IMC or any other SNMP management station; controller supports SNMPv3 as well as SSH and SSL for secure CLI and Web management

• Support for environments using Bonjour services

– Gateway: Allows discovery of Bonjour services located in a different layer-3 network

– HP Zerocast: Eliminates Bonjour multicast traffic from the WLAN enabling scalable deployment of Apple devices with no performance impact on the Wi-Fi network

– Access control: Enables filters to be applied inbound and outbound (on the AP) to SSIDs, groups of or specific APs. User based filtering can block Bonjour traffic until the user is authenticated

- VLAN pooling

  enables wireless clients to be dynamically assigned to different VLANs so administrators can assign different subnets to different clients in the same SSID. A VLAN pool can bind to multiple SSIDs

- Unified network visibility

  provides visibility between a wired and wireless network using IEEE 802.1AB Link Layer Discovery Protocol (LLDP) and sFlow

- AP Plug and Play (PnP)

  provides zero-configuration capability. An AP without a predefined configuration file can connect to the WLAN controller and the WLAN Controller will provision it with the correct wireless configuration

- Policy based forwarding

  simplifies the deployment of centralized or local forwarding. The policy-based mode allows user to classify data traffic based on ACL and choose local or centralized forwarding. Policy-based forwarding can be applied based on SSID or user-profile. That means a forwarding policy can be applied on a SSID or a specific user or a group of users

- AP grouping

  enables an admin to easily apply AP-based or radio-based configurations to all the AP that are in the same group

- Staged Firmware Upgrades

  enables an admin to selectively upgrade APs, typically a group of APs, to minimize the impact of upgrading large deployments of APs to a new version of firmware

- Custom antenna settings

  allow the admin to select a custom antenna gain

Quality of Service (QoS)

- End-to-end QoS

  the HP 10500/7500 20G Unified Wired-WLAN TAA-compliant Module supports the DiffServ standard and IPv6 QoS; the QoS DiffServ model includes traffic classification and traffic policing, and fully implements six groups of services—EF, AF1 through AF4, and BE

- IEEE 802.1p prioritization

  delivers data to devices based on the priority and type of traffic

- Class of Service (CoS)

  sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ

Security

- Web-based authentication

  provides a browser-based environment to authenticate clients that do not support the IEEE 802.1X supplicant

- IEEE 802.1X and RADIUS network logins

  support port-based and SSID-based 802.1X authentication and accounting

- WEP, WPA2, or WPA encryption

  can be deployed at the AP to lock out unauthorized wireless access by authenticating users prior to granting network access; robust Advanced Encryption Standard (AES) or Temporal Key Integrity Protocol (TKIP) encryption secures the data integrity of wireless traffic

- Secure shell

  encrypts all transmitted data for secure remote CLI access over IP networks

- Media access control (MAC) authentication

  provides simple authentication based on a user's MAC address; supports local or RADIUS-based authentication

- Integrated Wireless Intrusion Detection System (WIDS)

  support provides support for hybrid and dedicated modes; detects flood, spoofing, and weak IV attacks; displays statistics (events) and history; supports configuration of detection policies

- Integrated Wireless Intrusion Prevention System (WIPS)

  automatically identifies and classifies all APs and stations; enables packet-trigger containment via knowledge-based heuristics; protects against honeypot attacks and enforces STA security; detects Denial of Service (DoS) attacks via pre-defined DoS attacks, and provides a Signature mechanism which allows admins to define custom rules; enables Virtual Service Domains to deploy security policies by department or location for example

- Secure user isolation

  virtual AP services enable the network administrator to provide specific services for different user groups, allowing effective resource sharing, and simplifying network maintenance and management

- Endpoint Admission Defense

  integrated wired and wireless Endpoint Admission Defense (EAD) helps ensure that only wireless clients who comply with mandated enterprise security policies can access the network, reducing threat levels caused by infected wireless clients and improving the overall security of the wireless network

- Public Key Infrastructure (PKI)

  used to control access

- Authentication, authorization, and accounting (AAA)

  uses an embedded authentication server or external AAA server for local users

- Secure access by location

  AP location-based user access control helps ensure that wireless users can access and authenticate only to preselected APs, enabling system administrators to control the locations where a wireless user can access the network

- Wireless Intelligent Application Aware Feature (WIAA)

  provides a user role based or SSID based firewall embedded in WLAN Controller via ACL-based packet filter firewall and ASPF firewall. Protect clients from outside attacks Restrict specific users from accessing specific network resources

- Source Address Validation Improvement (SAVI)

  records the wireless client's IP address and MAC address and at the next data traffic forwarding stage, SAVI will validate the client's IP address to prevent attacker spoofing other client's IP address

Connectivity

- IPv6
  - IPv6 host

    enables controllers to be managed and deployed at the IPv6 network's edge
  - Dual stack (IPv4 and IPv6)

    transitions customers from IPv4 to IPv6, supporting connectivity for both protocols
  - MLD snooping

    directs IPv6 multicast traffic to the appropriate interface, preventing traffic flooding
  - IPv6 ACL/QoS

    supports ACL and QoS for IPv6 network traffic
- NAT support
  - NAT traversal

    helps ensure that communication between a branch office AP and the module is supported when the branch is using NAT
  - Integrated NAT support

    replaces the private source IP address with a public address; enables multiple internal addresses to be mapped to the same public IP address; permits only certain internal IP addresses to be NATed, and provides an Application Layer Gateway that supports specific application protocols without requiring the NAT platform to be modified
- IEEE 802.3ad Link Aggregation Control Protocol (LACP)

  supports a total of a 128 trunk groups with each group supporting 8 active ports. Ports must be of the same type (that is, all 100/1000 ports or 10GbE ports)

Performance

- Flexible forwarding modes
  - enable distributed and centralized traffic forwarding

    centralized forwarding, wireless traffic is sent to the module for processing. With distributed mode wireless traffic is dropped off locally. In the event that connectivity to the module is lost, authenticated clients can continue to access local resources
  - support local drop off or centralization of data traffic

    after an HTML authentication using the built-in portal server or IMC portal authentication.
- Wireless user access control and management

  support defining settings such as Committed Access Rate (CAS), QoS profiles, and access control policies based on location for different applications
- Fast roaming

  supports Layer 3 roaming and fast roaming, satisfying the most demanding voice service requirements
- Robust switching capacity and wire-speed processing

  deliver powerful forwarding capacity to support large enterprise WLANs

Resiliency and high availability

- High reliability

  The module supports 1+1, N+1, and N+N backup; the 1+1 redundancy configuration of the modules supports subsecond-level failure detection; APs establish AP-module tunnel links with both modules, but only the links to the active module are active; when the active module fails, the heartbeat mechanism between the two modules helps ensure that the standby module can sense the failure in subsecond level and then informs the APs to switch over to it, thus providing service continuity
- 802.1X hot-backup

  enables two controllers to sync 802.1X state information and wireless client's 802.11 information from master to backup. This feature is only supported on the HP 850, HP 870 and 20G Unified Module

Layer 2 switching

- VLAN support and tagging

  supports IEEE 802.1Q with 4,094 simultaneous VLAN IDs
- Jumbo packet support

  supports up to 4 KB frame size to improve the performance of large data transfers

Comprehensive portfolio

• Access point support

Refer to the HP Access Point—Controller Compatibility Matrix (h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-0345ENW&cc=us&lc=en).

Scalability

• Ease of deployment

these wireless interface cards use the backplane for all network and management communications, with no need for external network power connections

• Optional 32 or 128 access-point upgrade license

allows you to increase support for additional access points from the base 128 AP support without the need to buy additional costly hardware and use additional valuable space in a chassis; a redundant module must be provisioned with the same number of APs as the primary module. A special reduced-cost 128-access point license is available for use on the redundant module. Refer to the Specifications and Accessories sections for more detail

Warranty and support

• 1-year warranty

advance hardware replacement with 10-calendar-day delivery (available in most countries)

• Electronic and telephone support

1-year limited electronic and telephone support is available from HP; to reach our support centers, refer to hp.com/networking/contact-support; for details on the duration of support provided with your product purchase, refer to hp.com/networking/warrantysummary

• Software releases

includes all offered software releases for as long as you own the product; to find software for your product, refer to hp.com/networking/support; for details on the software releases available with your product purchase, refer to hp.com/networking/warrantysummary

HP 10500/7500 20G Unified Wired-WLAN TAA-compliant Module

Specifications

	HP 10500/7500 20G Unified Wired-WLAN TAA-compliant Module (JG645A)
I/O ports and slots	1 RJ-45 serial console port (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only 1 RJ-45 out-of-band management port (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only
Physical characteristics	
Dimensions	15.71(w) x 13.98(d) x 1.57(h) in (39.9 x 35.5 x 4.0 cm) (1U height)
Weight	7.98 lb (3.62 kg)
Memory and processor	
Processor	Eight core @ 950 MHz, 1 GB compact flash, 2 GB DDR2 DIMM
Performance	
Switch fabric speed	20 Gb/s
MAC address table size	24000 entries
Environment	
Operating temperature	32°F to 113°F (0°C to 45°C)
Operating relative humidity	5% to 95%, noncondensing
Nonoperating/Storage temperature	-40°F to 158°F (-40°C to 70°C)
Nonoperating/Storage relative humidity	5% to 95%, noncondensing
Electrical characteristics	
Maximum heat dissipation	512 BTU/hr (540.16 kJ/hr)
Maximum power rating	150 W
	Note Power consumption: 118 W-150 W
Safety	UL 60950-1; CAN/CSA 22.2 No. 60950-1; IEC 60950-1; EN 60950-1; FDA 21 CFR Subchapter J
Emissions	EN 55022 Class A; CISPR 22 Class A; ICES-003 Class A; AS/NZS CISPR 22 Class A; EN 61000-3-2; EN 61000-3-3; VCCI-3 CLASS A; VCCI-4 CLASS A; ETSI EN 300 386; FCC Part 15 (CFR 47) CLASS A

	HP 10500/7500 20G Unified Wired-WLAN TAA-compliant Module (JG645A)
Immunity	
EN	EN 55024, CISPR24 & ETSI EN 300 386
Management	IMC—Intelligent Management Center; command-line interface; Web browser; SNMP Manager; Telnet; HTTPS; RMON1; FTP; in-line and out-of-band; IEEE 802.3 Ethernet MIB; Ethernet Interface MIB
Features	For use in HP 11900, 10500 and HP 7500 Switch Series Default supported APs: 128 Maximum supported APs: 1,024 (via the optional purchase of the 32 and 128-Access Points E-LTU) Maximum supported clients and centralized throughput: • 20,000 clients • 20G of centralized throughput Maximum supported users via local portal authentication: 4,000 Maximum supported users via local authentication: 1,000 Maximum supported configured SSIDs: 512 Maximum supported ACLs: 32,000 Supported MSM APs are automatically discovered, Comware firmware is loaded, and the APs can be fully managed. AP upgrade license rules for redundant HP 10500/7500 20G Unified Wired-WLAN Module deployments • The primary HP 10500/7500 20G Unified Wired-WLAN Module's AP count must be increased using the optional HP Unified Wired-WLAN 128 AP E-LTU (JG649AAE) or HP Unified Wired-WLAN 32 AP E-LTU (JG774AAE). • The secondary HP 10500/7500 20G Unified Wired-WLAN Module's AP count can be increased as needed using the reduced-cost HP Unified Wired-WLAN 128 AP Redundant E-LTU (JG902AAE).
Notes	The faceplate of the HP 10500/7500 20G Unified Wired-WLAN TAA-compliant Module uses LSU3WCMD0 as the unique product identifier instead of JG645A.
Services	Refer to the HP website at hp.com/networking/services for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local HP sales office.

Standards and Protocols
(applies to all products in series)

General protocols	RFC 768 UDP RFC 791 IP RFC 792 ICMP RFC 793 TCP RFC 826 ARP RFC 854 TELNET RFC 855 Telnet Option Specification RFC 858 Telnet Suppress Go Ahead Option RFC 894 IP over Ethernet RFC 950 Internet Standard Subnetting Procedure RFC 959 File Transfer Protocol (FTP) RFC 1122 Host Requirements RFC 1141 Incremental updating of the Internet checksum	RFC 1144 Compressing TCP/IP headers for low-speed serial links RFC 1256 ICMP Router Discovery Protocol (IRDP) RFC 1305 NTPv3 (IPv4 only) RFC 1321 The MD5 Message-Digest Algorithm RFC 1334 PPP Authentication Protocols (PAP) RFC 1350 TFTP Protocol (revision 2) RFC 1519 CIDR RFC 1812 IPv4 Routing RFC 1944 Benchmarking Methodology for Network Interconnect Devices RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP) RFC 2104 HMAC: Keyed-Hashing for Message Authentication	RFC 2246 The TLS Protocol Version 1.0 RFC 2284 EAP over LAN RFC 2644 Directed Broadcast Control RFC 2864 The Inverted Stack Table Extension to the Interfaces Group MIB RFC 2866 RADIUS Accounting RFC 2869 RADIUS Extensions RFC 3164 Syslog RFC 3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS) RFC 3619 Ethernet Automatic Protection Switching (EAPS) RFC 3636 Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)
IP multicast	RFC 1112 IGMP	RFC 2236 IGMPv2	RFC 2934 Protocol Independent Multicast MIB for IPv4
IPv6	RFC 1350 TFTP RFC 1881 IPv6 Address Allocation Management RFC 1887 IPv6 Unicast Address Allocation Architecture RFC 1981 IPv6 Path MTU Discovery RFC 2292 Advanced Sockets API for IPv6 RFC 2373 IPv6 Addressing Architecture RFC 2375 IPv6 Multicast Address Assignments RFC 2460 IPv6 Specification RFC 2461 IPv6 Neighbor Discovery RFC 2462 IPv6 Stateless Address Auto-configuration RFC 2463 ICMPv6 RFC 2464 Transmission of IPv6 over Ethernet Networks	RFC 2465 Management Information Base for IP Version 6: Textual Conventions and General Group (partially support, only "IPv6 Interface Statistics table") RFC 2466, Management Information Base for IP Version 6 - ICMPv6 RFC 2526 Reserved IPv6 Subnet Anycast Addresses RFC 2553 Basic Socket Interface Extensions for IPv6 RFC 2563 ICMPv6 RFC 2925 Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations (Ping only) RFC 3315 DHCPv6 (client and relay) RFC 3363 DNS support RFC 3484 Default Address Selection for IPv6	RFC 3493 Basic Socket Interface Extensions for IPv6 RFC 3513 IPv6 Addressing Architecture RFC 3542 Advanced Sockets API for IPv6 RFC 3587 IPv6 Global Unicast Address Format RFC 3596 DNS Extension for IPv6 RFC 4193, Unique Local IPv6 Unicast Addresses RFC 4443 ICMPv6 RFC 4541 IGMP & MLD Snooping Switch RFC 4861 IPv6 Neighbor Discovery RFC 4862 IPv6 Stateless Address Auto-configuration RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
MIBs	RFC 1213 (MIB-II) RFC 1229 Interface MIB Extensions RFC 1643 Ethernet MIB RFC 1757 Remote Network Monitoring MIB RFC 2011 SNMPv2 MIB for IP RFC 2012 SNMPv2 MIB for TCP	RFC 2013 SNMPv2 MIB for UDP RFC 2571 SNMP Framework MIB RFC 2572 SNMP-MPD MIB RFC 2613 SMON MIB RFC 2665 Ethernet-Like-MIB	RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual Extensions RFC 2863 The Interfaces Group MIB RFC 2932IP (Multicast Routing MIB) RFC 2933 IGMP MIB
Mobility	IEEE 802.11a High Speed Physical Layer in the 5 GHz Band IEEE 802.11ac WLAN Enhancements for Very High Throughput IEEE 802.11b Higher-Speed Physical Layer Extension in the 2.4 GHz Band IEEE 802.11d Global Harmonization IEEE 802.11e QoS enhancements	IEEE 802.11g Further Higher Data Rate Extension in the 2.4 GHz Band IEEE 802.11h Dynamic Frequency Selection IEEE 802.11i Medium Access Control (MAC) Security Enhancements IEEE 802.11n WLAN Enhancements for Higher Throughput IEEE 802.11s D1.06 draft	HotSpot 2.0 Release 1 per the WiFi Alliance Hotspot 2.0 (Release 1) Technical Specification Package v1.0.0 (refer to the HP Access Point—Controller Compatibility Matrix for certified APs) **Note** Some of the above standards are now included in IEEE 802.11-2012

Standards and Protocols
(applies to all products in series)

Network management	IEEE 802.11k-2008 (beacon measurement functionality used as part of radio resource management) RFC 1155 Structure of Management Information	RFC 1905 SNMPv2 Protocol Operations RFC 2573 SNMPv3 Applications RFC 2574 SNMPv3 User-based Security Model (USM)	RFC 2575 VACM for SNMP SNMPv1/v2c
QoS/CoS	RFC 2474 DS Field in the IPv4 and IPv6 Headers RFC 2474 DSCP DiffServ	RFC 2475 DiffServ Architecture RFC 3168 The Addition of Explicit Congestion Notification (ECN) to IP	Call Admission Control (CAC): supports client-based and channel-utilization based call admission policies Wi-Fi MultiMedia (WMM), IEEE 802.11e
Security	IEEE 802.11w Protected Management Frames IEEE 802.1X Port Based Network Access Control PEAP-GTC PEAP-MSCHAPv2 RFC 1851 ESP Triple DES Transform RFC 2246 Transport Layer Security (TLS) RFC 2401 Security Architecture for the Internet Protocol RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP) RFC 2409 The Internet Key Exchange (IKE)	RFC 2548 Microsoft Vendor-specific RADIUS Attributes RFC 2716 PPP EAP TLS Authentication Protocol RFC 2865 RADIUS Authentication RFC 2867 RADIUS Accounting Modifications for Tunnel Protocol Support RFC 3394 Advanced Encryption Standard (AES) Key Wrap Algorithm RFC 3576 Dynamic Authorization Extensions to RADIUS (Disconnect Message and Session-time renewal) RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)	RFC 3580 IEEE 802.1X RADIUS Guidelines Access Control Lists (ACLs) Guest VLAN for 802.1x Secure Sockets Layer (SSL) SSHv2 Secure Shell Web Authentication WPA (Wi-Fi Protected Access)/WPA2
VPN	RFC 2403 The Use of HMAC-MD5-96 within ESP and AH RFC 2404 The Use of HMAC-SHA-1-96 within ESP and AH	RFC 2405 The ESP DES-CBC Cipher Algorithm With Explicit IV	RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP RFC 2451 The ESP CBC-Mode Cipher Algorithms
IPSec	RFC 1829 The ESP DES-CBC Transform	RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPSec	
IKEv1		RFC 3748 - Extensible Authentication Protocol (EAP)	
PKI		RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	

HP 10500/7500 20G Unified Wired-WLAN TAA-compliant Module accessories

License	HP Unified Wired-WLAN 128 AP E-LTU (JG649AAE) HP Unified Wired-WLAN 128 AP Redundant E-LTU (JG902AAE) HP Unified Wired-WLAN 32 AP E-LTU (JG774AAE)

Learn more at
hp.com/networking

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

© Copyright 2013–2015 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Bluetooth is a trademark owned by its proprietor and used by Hewlett-Packard Company under license. Microsoft is a U.S. registered trademark of the Microsoft group of companies.

4AA4-6469ENW, February 2015, Rev. 7